Defense Civilian Pay System (DCPS) Security Awareness

Janette Norris
Information Systems Security Officer (ISSO), Civilian Pay Services

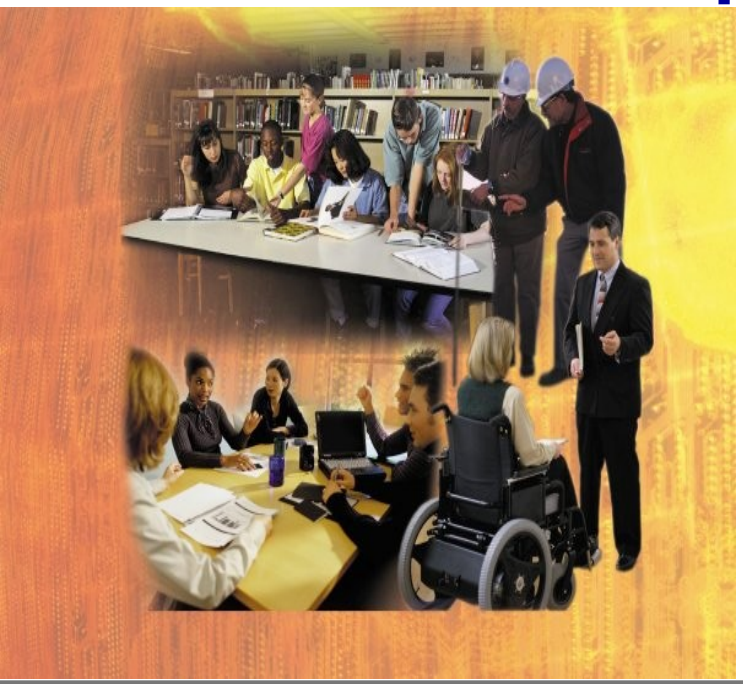
December 2003

Your Financial Partner @ Work

Information Protection

WHAT IS OUR JOB?

To protect information and system resources against all occurrences of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse or release to unauthorized persons.



Security Foundation is based on:

- **Confidentiality**
- **Integrity**
- **Availability**

Freedom of Information Act

Enacted in 1966 to provide universal access to official information.

Categories that are exempt from FOIA:

- Classified information
- Internal rules and practices
- Information denied by other specific withholding statutes
- Trade secrets and commercial or financial information given in confidence
- Inter and Intra-Agency communication
- Personal information protected by the Privacy Act
- Investigative information compiled for la enforcement
- Reports on financial institutions

For additional information on FOIA:

http://www.defenselink.mil/pubs/foi

Public Law 93-579, 5 U.S.C §

Privacy Act of 1974

- **Virtually all data within DCPS contains sensitive unclassified information that is subject to protection from disclosure under the Privacy Act of 1974**
- **Examples of DOD civilian privacy information not releasable to the public:**

Date of Birth	**Home Address**
Home Tel. No.	**Home E-Mail**
Net Salary	**Deductions**
Debts	**Leave Balances**

IT IS YOUR RESPONSIBILITY TO PROTECT ANY CIVILIAN EMPLOYEE FINANCIAL INFORMATION THAT YOU PROCESS.

Terminal User

While at your terminal:

- Protect your password, do NOT write it down and do NOT divulge it to anyone
- Use only the userid and password you were assigned
- Protect your keyboard and screen while entering your password
- Do NOT leave your terminal unattended while logged into DCPS, log off or lock it

If your password is compromised, notify your servicing Payroll Office Security Team immediately.

Individual Accountability

DCPS accounts are issued for the performance of official duties only; any other use is strictly prohibited.

- **Users cannot access their own records**
- **Users are accountable for their actions when they sign the Security Access Questionnaire form**
- **Security Awareness is accountable when a user sends course completion acknowledgment to the ISSO**

Security Incident Reporting

Report ALL suspicious activity to the DCPS Information System Security Office via email

- **Information to report:**
  - **Date and Persons involved**
  - **Full description of the incident**
  - **Any action taken**

Send e-mail to: fpe-dcps-isso@dfas.mil

Monitoring / Audit Trails

DCPS writes all transactions to journal logs

- **Actions taken via your login ID are subject to being monitored and are logged.**

- **Audit trails are used to detect and deter penetration of DCPS and to reveal usage that identifies misuse.**

Policy- Implications of Non-

DCPS users are required to comply with policy and violations may result in appropriate disciplinary action.

Violations may also result in penalties under criminal, civil, military statutes, and the Uniform Code of Military.

DCPS CBT TRAINING

Location:
https://dfas4dod.dfas.mil/systems/dcps/consolid/cbt/cbttoc.htm

- **Security Awareness CBT *(mandatory)***
- **Online Time & Attendance CBT**
- **CSR Employee Data Collection CBT**
- **Enhanced CSR CBT**

For assistance: call (850) 453-4141, x310 or email: fpe.customer.contact.center@dfas.mil

Questions?